UNITED STATES MARINE CORPS
MARINE CORPS LOGISTICS BASES
814 RADFORD BOULEVARD
ALBANY, GEORGIA 31704-0323

IN REPLY REFER TO:
2000
G600

MAR 18 2002

POLICY STATEMENT 3-02

From: Commander
To: Distribution List

Subj: INTERNET USE POLICY

Ref: (a) IRM 5239-08 Computer Security Procedures
(b) IRM 5239-10 Small Computer Security
(c) Public Law 99-474 (Computer Fraud and Abuse Act of 1986)
(d) Title 17 of the U.S. Code (Sections 106 and 117)
(e) Title 18 of the U.S. Code (Sections 1030 and 2319)
(f) BO P12000.6A – Civilian Personnel Manual
(g) UCMJ – Uniform Code of Military Justice
(h) MARADMIN 162-00

1. Purpose. To establish policy and emphasize the need for increased vigilance and care in the use of a government-owned personal computer when accessing the Internet. To identify all permissible and non-permissible uses of the Internet, via a government-owned resource, consistent with the legal and security rules described below and in references (a) through (h).

2. Background. To ensure that our resources are consistently available, we must use the resources in a professional manner. Inappropriate use causes the following problems:

a. Information Technology (IT) resources are wasted. Many of today's web applications consume tremendous amounts of network bandwidth. Accessing for personal rather than official Marine Corps business decreases the amount of bandwidth that is available for work-related activities. Decreased bandwidth results in slow network performance and a need for costly network upgrades.

b. Network security is compromised. When data is downloaded from inappropriate web sites, they provide an easy way for hostile code to slip past our network firewall protection system and infiltrate our computer systems. Many of these inappropriate web sites will monitor "your traffic" and capture data such as password, IP address, and user name. The hacker can then use this captured information to break into our network.

c. Productivity suffers. Every minute a user spends on the Internet viewing or performing functions such as online stock trading, online auctions, sports sites, gambling, pornography, and online gaming, is a minute not spent doing the work they are supposed to be doing. The official work does not get accomplished, deadlines are missed, and productivity suffers.

d. Liability risk increases. The downloading or distribution of adult or other inappropriate content over the Internet can expose other users to objectionable material. This then puts the Marine Corps at risk of lawsuit by creating a hostile environment where sexual harassment and other illegal activities can take place.

3. Policy

a. Permissible uses of the Internet are defined to include Official use and Authorized use.

(1) Official use: Marine Corps IT resources (i.e. computer hardware, software and telecommunications infrastructure) can be used when work-related and determined to be in the best interests of the federal government and the Marine Corps. Access should be appropriate in frequency, duration, and be related to assigned tasks. Examples include using the Internet to:

(a) Obtain information to support DoD/DoN/USMC missions

(b) Obtain information that enhances the professional skills of Marine Corps personnel

(c) Improve professional or personal skills as part of a formal academic education or military/civilian professional development program (if approved by the Command).

(2) Authorized use: Marine Corps resources may be used to access the Internet for incidental personal purposes such as Internet searches and brief communications as long as such use:

(a) Does not adversely affect the performance of official duties by the Marine/employee, and his/her supervisor permits it

(b) Serves a legitimate public interest such as enhancing professional skills

(c) Is of minimal frequency and duration, and occurs during an individual's personal time

(d) Does not overburden Marine Corps computing resources or communication systems

(e) Does not result in added costs to the government

(f) Is not used for purposes that adversely reflect upon the Marine Corps

b. Prohibited use: Use of Marine Corps resources to connect to the Internet for purposes other than those described in paragraph 3.a. above is prohibited. Examples of prohibited use include, but are not limited to, the following:

(1) Accessing the Internet without first reading and agreeing to the requirements addressed in the Logon Warning Banner

(2) Illegal, fraudulent, or malicious activities

(3) Introducing classified information into an unclassified hardware or software system

(4) Accessing, storing, processing, displaying, distributing, transmitting, or viewing offensive or obscene material that is pornographic, racist, promotive of hate groups or hate crimes, or subversive in nature

(5) Storing, accessing, processing, or distributing classified, proprietary, sensitive but unclassified (SBU), For Official Use Only (FOUO), or privacy act-protected information in violation of established security and information release policies.

(6) Obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the vendor's patent, copyright, trade secret, or license agreement.

(7) Knowingly writing, coding, compiling, storing, transmitting, or transferring malicious software code to include viruses, logic bombs, Trojan horses, worms, and macro viruses

(8) Promoting partisan political activity that violates the Hatch Act

(9) Disseminating unsolicited religious material outside an established command-sponsored religious program

(10) Activities that are used for purposes of personal or commercial financial gain - These activities include solicitation of business services or sale of personal property. Examples are on-line auction and the selling or buying of personal stock or portfolios. Exceptions are a command-approved mechanism such as a welfare and recreation bulletin board, the Thrift Saving Plan, or Command-sponsored payment or retirement systems

(11) Gambling, wagering, or placing of any bets, to include sporting activity pools

(12) Downloading or participating in any on-line Internet games

(13) Posting personal home pages

(14) Access and use of unofficial streaming audio and video web sites, i.e. listening to radio stations and broadcast online

(15) Encryption of personal electronic communications

(16) Using the Command-sponsored Internet access as an Internet Service Provider for personal use

(17) Fund-raising activities, either for profit or non-profit, unless the activity is sponsored by the Command

c. All users are reminded that they have no expectation of privacy when using government computer resources. Use of government computer resources, including use of Email and browsing the World Wide Web, is subject to monitoring, interception, accessing, and recording, and may be passed to law enforcement officials.

d. Naval Criminal Investigative Service has an active computer crime and counterintelligence team at MCLB Albany. Commanding officers should contact the Information Systems Security Manager whenever it is discovered that a government information system is being used for criminal or foreign intelligence purposes or is being invaded/probed by an unauthorized user.

e. The downloading of large mission-essential files in excess of 3 megabytes from the Internet will be limited to off-peak hours. Files of ".exe" or ".com" configuration will be scanned using the approved virus protection software prior to executing on any computer hard drive or disk drive. All files downloaded from the Internet become government property.

f. At no time will a government computer that is connected to the Marine Corps Enterprise Network also be simultaneously connected to a commercial Internet Service Provider (ISP) via a modem. Doing so would provide direct access for a hacker to enter the Marine Corps network.

g. Commanding officers have the authority to control or limit the use of government-owned resources for the purposes of security, morale, good order, discipline and to promote the efficiencies of their command. Commanders are to ensure that appropriate command level measures are instituted to:

(1) Control access of Internet services for those personnel required to use the Internet in performance of the Command's mission.

(2) Monitor local network usage and take appropriate action when inappropriate use is suspected.

(3) Investigate any unauthorized use and, where warranted, hold individuals accountable for unauthorized or inappropriate Internet use.

(4) Monitor local network utilization to ensure processing and network resources are not adversely impacted by Internet use. Specific attention should be placed on Internet applications and services that are bandwidth intensive and have a cumulative detrimental effect on telecommunications infrastructure (e.g., Point Cast, Cuseeme, etc.). When required, take action to prevent degradation to include restricting access to specific Internet sites or network resources. Commands are authorized to place time limits on when certain types of web sites are available for access.

(5) Educate personnel on appropriate Internet activity and access.

4. Administrative Actions. Failure to abide by this policy will result in administrative or punitive action. This may include loss of account access.

5. Point of Contact. Address questions concerning Information Assurance to MARCORLOGBASES AC/S, G6, Information Technology Department, Information Assurance Office (G620) at DSN 567-7133 or Commercial (229)-639-7133. Email is matcomg6iaoffice@matcom.usmc.mil. Information can also be obtained from the MARCORLOGBASES G6 Information Assurance Office website at http://www.ala.usmc.mil/iao.

6. Applicability. This policy is applicable throughout all activities aboard MCLB Albany, MCLB Barstow, and Blount Island Command.

R.S. Kramlich
R. S. KRAMLICH

Distribution: A